ПРИВАТНОСТЬ

Антикриминалистика. Как защитить смартфон от извлечения данных

Олег Афонин , только что 14 мин на чтение 0 0 127



Мобильная версия статьи

Содержание статьи

Своеобразным триггером, вызвавшим появление этой статьи, стало огромное количество публикаций в самых разнообразных изданиях, в том числе достаточно технических. Все эти публикации без единого исключения уныло повторяют одну и ту же мантру: используйте стойкий код блокировки, включите датчик отпечатков, отключите Smart Lock, включите двухфакторную аутентификацию, обновитесь на последнюю доступную версию ОС… Не будем спорить, все эти вещи проделать необходимо — но совершенно, абсолютно недостаточно.

Ты можешь выбрать самый стойкий код блокировки, но если в твоем телефоне используется шифрование FDE и ты не включил режим Secure Startup, то код блокировки может быть хоть в сотню символов длиной — шифрование все равно будет использовать фразу default_password. Отключение Smart Lock — необходимый, но недостаточный шаг; уверен ли ты в безопасности используемой в твоем устройстве технологии сканирования лица (если телефон ей оборудован)? А знаешь ли ты, что, просто зайдя на твой компьютер, можно извлечь все твои облачные пароли, после чего попросту сбросить код блокировки смартфона? (Работает, к счастью, не для всех устройств, но знать о такой возможности нужно.) Наконец, нужно отдавать себе отчет, что если с твоего компьютера будет получен пароль от облака (Google, Apple или Samsung), то сам телефон будет никому не нужен: все необходимые данные эксперт извлечет из облака (и, скорее всего, их там будет даже больше, чем в самом телефоне).

В данной статье мы не будем давать набивших оскомину советов «включить код блокировки» или «обновиться до последней версии ОС» (разумеется, ты это уже сделал). Вместо этого мы постараемся дать понимание всего спектра возможностей «тяжелой артиллерии», которая может быть использована против владельца телефона правоохранительными органами и спецслужбами для извлечения данных.

Как известно, самые сложные для работы экспертов случаи — обесточенный телефон, обнаруженный у безмолвного тела. Именно в таких обстоятельствах, как правило, начинается поиск всевозможных уязвимостей в программном и аппаратном обеспечении. В обыденных ситуациях полиция придет домой к подозреваемому, проведет анализ компьютера и извлечет кеш паролей из почтовых клиентов и браузеров Chrome/Mozilla/Edge. Затем достаточно зайти в облако с найденным логином и паролем, после чего остальное тривиально. В ряде случаев на телефоне можно удаленно сбросить пароль блокировки (сегодня, к счастью, многие производители не предлагают такой возможности по умолчанию). Телефон можно подключить к «осьминогу» UFED, который скопирует раздел данных и расшифрует его через одну из известных разработчикам уязвимостей или с использованием «расшифровывающего загрузчика» (decrypting bootloader в терминах Cellebrite) независимо от длины твоего пароля и наличия установленных обновлений.

Прочитав эту статью, ты будешь более полно осознавать возможности защитить свои данные и риски, которые останутся даже тогда, когда ты все сделал правильно.

Как будут взламывать твой iPhone

Сложность взлома iPhone отличается в зависимости от ряда факторов. Первый фактор: установленная версия iOS (ты ведь не думаешь, что советы «обновиться на последнюю доступную версию» появились на ровном месте?), сложность кода блокировки и то, в каком состоянии находится устройство (о нем — ниже).

Сначала — о версиях iOS. Если у тебя до сих пор установлена любая версия iOS 11, у меня для тебя плохая новость: для этой ОС доступен как взлом кода блокировки методом прямого перебора, так и полное (и очень быстрое) извлечение информации через физический доступ. Сложность кода блокировки и состояние устройства (включено-выключено, активирован ли защитный режим USB restricted mode и так далее) повлияют на скорость перебора.

Как будут взламывать iPhone с iOS 11

Если телефон был выключен: скорость перебора паролей будет очень медленной (одна попытка в десять секунд). Если ты установишь код блокировки из шести цифр, то перебирать его будут вечность.

Если телефон был включен и ты хотя бы раз разблокировал его после включения: первые 300 000 паролей будут опробованы очень быстро; скорость перебора такова, что четырехзначный код блокировки может быть взломан в течение получаса в полностью

автоматическом режиме. Вывод? Используй шестизначный пароль.

Если ты успел воспользоваться режимом SOS (зажав кнопку питания и кнопку громкости): телефон снова переходит в режим «медленного» перебора. Шестизначный код блокировки в этом случае отличная защита.

Наконец, в iOS 11.4.1 появился режим USB restricted mode, позволяющий защитить устройство от взлома путем перебора паролей. В течение часа после последнего разблокирования iOS отключит доступ к USB-порту, после чего перебор паролей станет невозможным. Для того чтобы защита сработала, нужно оставить переключатель USB Accessories в положении «выключено». Впрочем, в последнее время активно циркулируют слухи, что разработчикам криминалистических комплексов удалось или вот-вот удастся обойти и эту защиту. Вывод? Да обновись ты до iOS 12, наконец!

Как будут взламывать iPhone с iOS 12

Ситуация с iOS 12 довольно интересна. Apple удалось закрыть ряд уязвимостей, которые делали возможным перебор паролей на устройствах с iOS 11. Более того, защитный режим USB restricted mode был усовершенствован: теперь USB-порт (а точнее, возможность передачи данных через физический коннектор Lightning) отключается сразу же, как только ты заблокируешь экран устройства. Правда, только в тех случаях, если ты как минимум три дня не подключал телефон к компьютеру, проводной аудиосистеме или другим аксессуарам; если же подключал, то будет как раньше — через час. Кроме того, USB-порт теперь отключается и при вызове режима SOS (зажать кнопку питания и громкости).

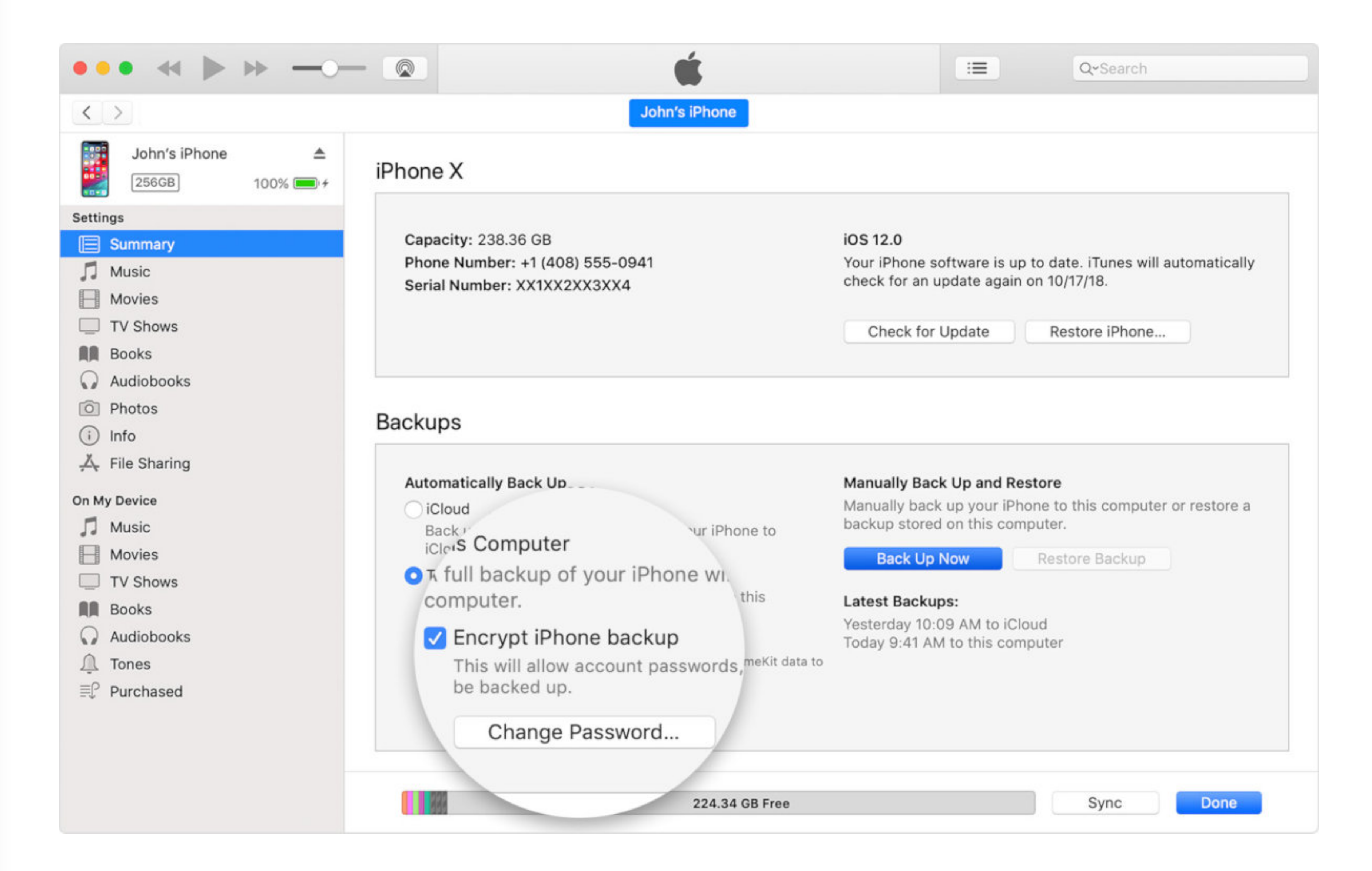
С другой стороны, в iOS 12 присутствуют уязвимости, перекочевавшие в систему еще из 11-й версии ОС. В iOS 12 вплоть до версии 12.1.2 не были закрыты две важные уязвимости, позволяющие через эскалацию привилегий получить полный доступ к файловой системе без установки полноценного джейлбрейка. Соответственно, если в руки экспертов телефон с iOS 12.1.2 или более старой попадет в разблокированном состоянии, то данные из него улетят со свистом. В iOS 12.1.3 часть уязвимостей была закрыта (не все: GrayKey по-прежнему способен извлечь образ файловой системы), но полностью обезопасить устройства от известных на сегодняшний день эксплоитов смогла только iOS 12.1.4, которая вышла буквально на днях. Вывод? В совете «обновись до последней доступной версии прошивки» все-таки что-то есть!

Итак, как именно будут пытаться взломать твой iPhone с iOS 12?

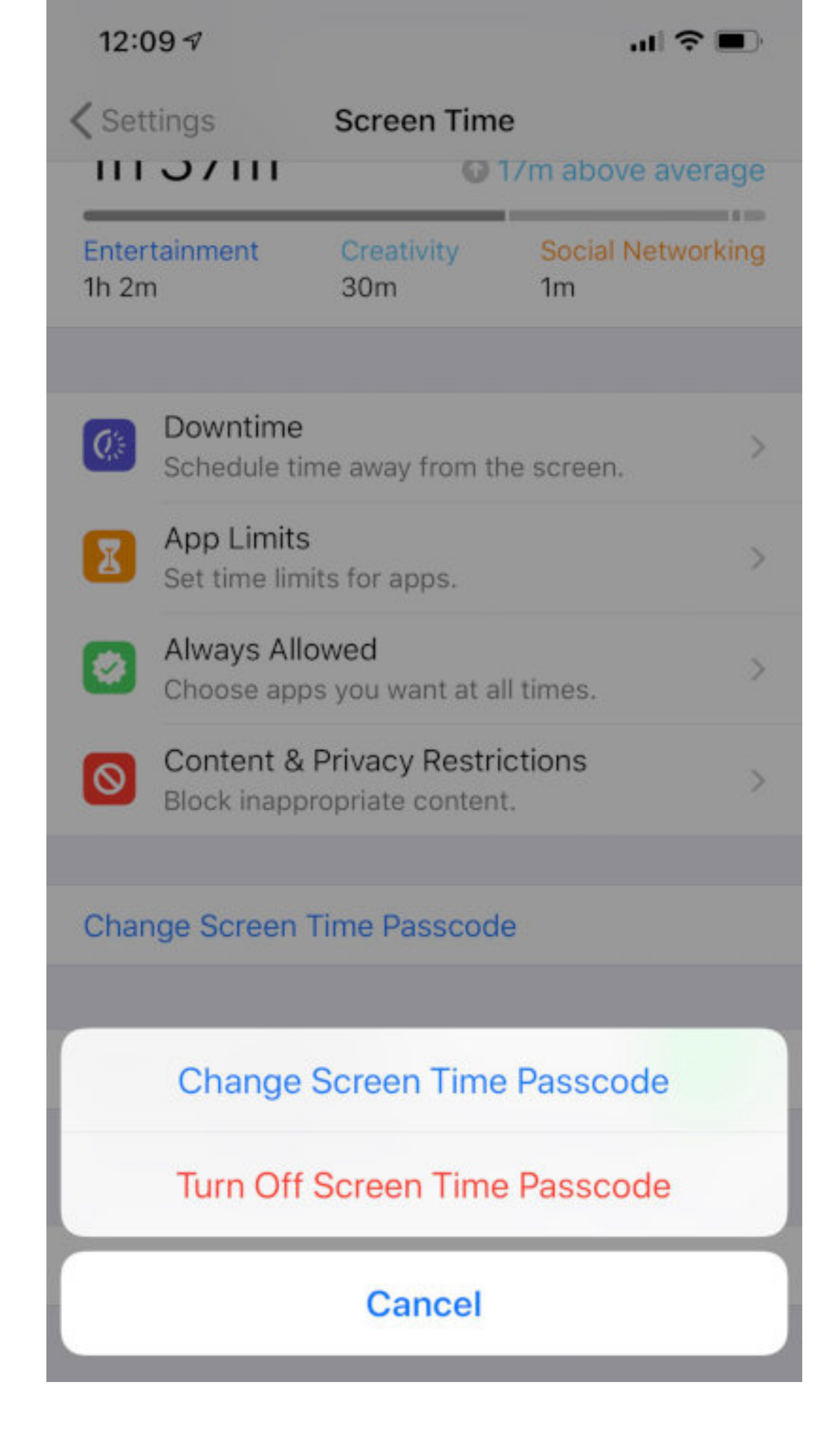
Самый безопасный для тебя вариант — если в руки эксперта твой телефон попадет в выключенном состоянии. В этом случае начать перебор не удастся — по крайней мере до тех пор, пока разработчики не придумают, как обойти защитный режим USB (к слову,

пока не придумали).

Если телефон был включен и разблокирован хотя бы раз после включения (но заблокирован на момент взлома), то сделать с ним что-то полезное тоже не получится. Да, можно попытаться подключить его к твоему компьютеру, чтобы создать резервную копию через iTunes; если не успел активироваться защитный режим USB и если ты хоть раз подключал свой iPhone к iTunes, то попытка может оказаться успешной. Как защититься? Установи длинный и сложный пароль на резервную копию.



Да, в iOS 12 (и в iOS 11) этот пароль можно сбросить — но только с самого iPhone и только если известен код блокировки. И даже тогда ты можешь дополнительно защитить пароль от сброса, установив пароль Screen Time.



Пароль Screen Time — не панацея. Вообще говоря, это «детская» защита, функция защиты от сброса пароля на резервную копию в ней вторична. Тем не менее обойти ее не получится даже перебором: iOS будет увеличивать задержки до тех пор, пока скорость перебора не упадет до одной попытки в час (начиная с десятой попытки).

Если забрали разблокированный телефон

В идеальном мире полиции пришлось бы проявить технические навыки и пользоваться блестящими устройствами, чтобы просто попытаться взломать твой смартфон. В большинстве же случаев полиция просто попытается извлечь из твоего смартфона максимум информации в рамках имеющихся полномочий за минимальное время. Уверенным голосом «попросить» разблокировать телефон, после чего унести разблокированный телефон в отдельную комнату — самый типичный случай для (не льсти себе) мелких правонарушителей. Давай посмотрим, что может сделать iOS для защиты твоих данных в этом случае.

Итак, вводная: iPhone разблокирован и передан сотруднику, но код блокировки ты не сообщал. (В скобках: и не сообщай, нет у тебя такой обязанности в случае обычного задержания.) Что будет происходить дальше?

Во-первых, сотрудник может просто вручную просмотреть интересующие его разделы в устройстве. Здесь и постинги в соцсетях (уверен, на тебя там ничего не найдут, но статья за лайки — она довольно гибкая), и переписка, и сообщения SMS/iMessage, и, разумеется, фотографии.

Будут извлечены данные приложения «Здоровье», из которых можно будет сделать выводы о том, что именно ты делал в тот или иной момент (в частности, будет видно — двигался ты или сидел на месте, а если двигался — то не бежал ли). Нам известен не один, не два и даже не десяток случаев, когда рутинное задержание вдруг превращалось в арест и предъявление обвинения по факту найденной в смартфоне информации.

Как защититься от анализа в этом режиме? Никак, только не передавать полиции разблокированное устройство. Не отдать телефон совсем ты не можешь, но вот отказаться его разблокировать — пока что еще твое право (исключения бывают, например при пересечении границы; мы про них писали). Здесь отметим, что даже на устройстве с разблокированным экраном без кода блокировки не удастся ни просмотреть пароли из «связки ключей», ни отключить Find My iPhone, ни сбросить пароль от резервной копии iTunes, если ты его установил, ни даже подключить телефон к компьютеру: для этого теперь тоже нужен код блокировки.

Во-вторых, телефон могут подключить к комплексу GrayKey или подобному (правда, «подобных» на самом деле нет, но мало ли? Вдруг китайские дубликаторы жестких дисков научатся взламывать iPhone?). В этом случае спасти может лишь свежая версия iOS: напомним, вплоть до iOS 12.1.3 включительно нет никакой проблемы с тем, чтобы извлечь из устройства образ файловой системы. В iOS 12.1.4 уязвимость была закрыта. Надолго ли? Пока неизвестно.

Наконец, из телефона могут попытаться извлечь данные в виде резервной копии. Для этого потребуется как минимум подключить телефон к компьютеру, для чего эксперту

понадобится код блокировки экрана. Можно попытаться обойти этот момент, используя файл lockdown из твоего компьютера. Впрочем, если ты установишь пароль на резервную копию и защитишь его от сброса при помощи пароля Screen Time, ты можешь полностью обезопасить себя с этой стороны.

Вывод? Если ты разблокировал iPhone и на телефоне установлена последняя версия iOS (на сегодня это 12.1.4), сотрудник, скорее всего, будет вынужден ограничиться «ручным» анализом на экране самого телефона.

Как будут взламывать твой смартфон на Android

Как и в случае с iPhone, в полиции попытаются заставить тебя разблокировать устройство. Если им это удастся и ты передашь в руки полиции разблокированный телефон, расслабься: дальнейшее от тебя не зависит; ты выдал все, что было можно. В отличие от iOS, которая пытается хоть как-нибудь защитить тебя даже в таких ситуациях, с экрана разблокированного смартфона следователь получит:

- разумеется, доступ ко всему содержимому карты памяти (виртуальной и реальной), включая фото и видео;
- почту, переписку в мессенджерах, тексты SMS;
- полный список паролей, сохраненных в Chrome (частенько там можно найти и пароль от твоего Google Account — кстати, проверь, так ли это);
- подробную историю местоположения. Очень подробную;
- данные Google Fit. Их можно экспортировать;
- звонки, контакты.

Взлом кода блокировки экрана

Мне очень хотелось бы написать подробную статью о том, как и чем можно взломать заблокированный смартфон на Android, но, боюсь, это невозможно: на руках у пользователей тысячи разнообразных моделей, основанных на десятках чипсетов в сотнях вариаций. С учетом разнообразия прошивок, версий самого Android и доступности актуальных патчей безопасности (та самая проблема фрагментации Android) сложилась ситуация, в которой даже крупнейший производитель криминалистических продуктов не знает, с какими устройствами работает их комплекс. «Попробуйте подключить» — стандартный ответ на вопрос, поддерживает ли комплекс X смартфон Y.

К примеру, простой вопрос: можно ли взломать код блокировки у конкретной модели

смартфона, а главное — нужно ли это делать или можно обойтись и так? Многочисленные статьи по безопасности в один голос рекомендуют устанавливать стойкий код блокировки, умалчивая о том, что примерно для каждого второго смартфона это совершенно бесполезно. Как определить, имеет ли смысл заморачиваться со сложным кодом блокировки или нужно копать в другую сторону?

Ответ связан с алгоритмом шифрования, используемого в конкретном устройстве. Как ты помнишь, все смартфоны, вышедшие с завода с Android 6 и более поздними версиями, обязаны зашифровать пользовательские данные к моменту окончания начальной настройки. Однако шифрование шифрованию рознь. В большинстве старых устройств используется так называемое полнодисковое шифрование Full Disk Encryption (FDE). В режиме FDE данные на пользовательском разделе зашифрованы посредством device credentials — ключа шифрования, который генерируется на основе некого аппаратного ключа и фразы default_password.

Да, именно так — default_password защищает все твои данные. И что же, все пропало? Любой желающий может взять и расшифровать информацию? Не совсем. Ключ шифрования генерируется внутри Trusted Execution Environment (TEE) в момент загрузки устройства; в качестве исходных данных участвует уникальный для каждого устройства ключ, который за пределы TEE не выходит. Если из телефона извлечь чип памяти и скопировать из него информацию, то расшифровать данные без ключа из TEE не удастся. Соответственно, для расшифровки информации потребуется не просто вытащить из телефона данные (например, через режим EDL), а еще и взломать TEE или подменить загрузчик. В принципе, такие «расшифровывающие загрузчики» (decrypting bootloader) существуют, например у Cellebrite для целого ряда моделей, а иногда и целых семейств моделей, объединенных общим чипсетом. Тем не менее для использования этой возможности понадобится специальный комплекс, который и извлечет данные.

Даже если в твоем телефоне используется устаревшая защита FDE, ты можешь надежно защитить свои данные, активировав режим Secure Startup. В этом режиме ключ шифрования будет перешифрован данными аппаратного ключа и твоего кода блокировки (вместо default_password). Недостаток у этого метода тоже есть: телефон просто не загрузится вплоть до момента ввода кода блокировки; если твой телефон случайно перезагрузится, то ты не сможешь даже ответить на звонок, пока телефон не загрузится до конца.

Этот недостаток полностью устранен в новой пофайловой схеме шифрования, получившей название File Based Encryption (FBE). Устройства, зашифрованные FBE, используют user credentials (код блокировки) для шифрования большей части информации, в том числе всех персональных данных. При этом исполняемые файлы приложений, а также некоторые базы данных, необходимые для загрузки устройства, будут зашифрованы посредством device credentials (то есть данных исключительно аппаратного ключа). Режима Secure Startup при использовании FBE нет за ненужностью.

Для расшифровки данных как устройств с FDE, использующих режим Secure Startup, так и устройств с FBE необходимо взломать код блокировки. Конкретные процедуры отличаются в зависимости от чипсета, но общий принцип один: подключиться к USB-порту и запустить процедуру перебора.

Разумеется, в телефонах есть встроенная защита от таких атак. Мы уже описывали Qualcomm TrustZone, в рамках которой работает Trusted Execution Environment (TEE). В ней могут запускаться только так называемые трастлеты (trustlets), своеобразные микроприложения, подписанные ключом, который проверяется самой TEE. Именно здесь реализована проверка пасскода (через сервис GateKeeper). GateKeeper, в свою очередь, на аппаратном уровне ограничивает скорость перебора паролей; быстро перебрать даже код из четырех цифр не получится, а шесть цифр можно перебирать до бесконечности. Именно GateKeeper не даст взломать телефон, когда включен Secure Startup или если используется шифрование FBE.

Если есть защита, то будут и попытки ее взломать. В частности, для процессоров Qualcomm до Snapdragon 821 включительно существует эксплоит, позволяющий запустить на выполнение собственный трастлет и обойти ограничение на скорость перебора. В реальности же разработчики криминалистических комплексов относятся к этой уязвимости как к зубной боли: с одной стороны, уязвимость существует, она мозолит глаза; заказчики ее хотят. С другой — воспользоваться ей очень трудно: для каждого устройства нужно писать свой код, подбирать смещения, тестировать… Если бы речь шла об iPhone, количество актуальных чипсетов которого можно пересчитать по пальцам одной руки, — поддержка уязвимости такого уровня была бы реализована еще вчера. Но сотни модификаций чипсетов, использующихся в смартфонах с Android (причем каждая модель, для которой нужно запускать процесс разработки, попадет в руки полиции в единичных экземплярах), делают такую разработку экономически нецелесообразной.

Для флагманских смартфонов на процессорах Qualcomm возможность вытащить данные через уязвимости выглядит приблизительно так:

- для старых устройств (до Snapdragon 821 включительно) с эксплоитами иногда можно взломать пасскод, если не установлен Secure Startup (способов обнаружено множество);
- для старых устройств с включенным Secure Startup либо с шифрованием FBE скорость перебора ограничена GateKeeper. Атака на «холодное» устройство (после перезагрузки или включения) практически не реализуется за исключением единичных популярных моделей (проблема «неуловимого Джо»);
- для новых устройств (со Snapdragon 835 и новее) недоступны эксплоиты EDL,

недоступен эксплоит TEE и даже в редких случаях, когда используется шифрование FDE, расшифровать содержимое раздела данных довольно непросто (но в отдельных случаях можно, эксплоиты существуют);
- наконец, для новых устройств (SD835 и новее), использующих шифрование FBE, никакие эксплоиты не работают: ключ шифрования зависит от пароля, а перебор очень медленный (GateKeeper).

Как защитить свой смартфон от взлома кода блокировки и физического извлечения данных

Для начала проверь, какая система шифрования используется на твоем устройстве. Для этого выполни через ADB следующую команду:

```
$ adb shell getprop ro.crypto.type
```

Если команда вернула слово file, то твой смартфон использует шифрование FBE. Если используется пофайловое шифрование FBE:

- установи код блокировки длиной не менее шести цифр (если позволяет устройство);
- отключи отладочный режим USB Debugging.

Если используется FDE, включи Secure Startup. Для этого:

- зайди в настройки и удали текущий код блокировки;
- создай новый код блокировки. Система запросит, хочешь ли ты включить режим безопасной загрузки. Подтверди запрос;
- не забудь отключить отладочный режим USB Debugging.

Можно ли изменить тип шифрования с FDE на FBE? В общем случае — нет. Возможность перейти с FDE на FBE была лишь у некоторых устройств Google (например, в планшете Pixel C), когда FBE разрабатывался. Для современных устройств такой возможности нет.

Общие рекомендации

Какие рекомендации обычно дают статьи, посвященные безопасности Android? Использовать код блокировки посложнее или паттерн подлиннее; отключить Smart Lock;

обновить Android; включить двухфакторную аутентификацию. Советы звучат логично, но при этом исключительно поверхностно, в стиле «информационная безопасность для блондинок». Между тем для каждого второго смартфона на Android длина кода блокировки никак не влияет на безопасность; отключение Smart Lock бесполезно, если пользователь включил (или забыл выключить) отладочный режим USB debugging, а проверять обновления Android нет смысла, если производитель твоего устройства затягивает с обновлениями.

Для начала составим свой список рекомендаций, а потом пройдемся по некоторым пунктам подробно.

1. Код блокировки. Он нужен, и желательно не короче шести цифр. При этом следует проверить, какой механизм шифрования используется в твоем смартфоне — FDE или FBE, и если FDE, то необходимо включить режим безопасной загрузки Secure Startup.
2. Отключи отладочный режим USB debugging. Любые другие действия бессмысленны, если этот режим включен.
3. Наверное, ты в курсе, что разблокированный загрузчик — дыра в безопасности? Не будем даже рассматривать такие случаи, но если в настройках для разработчика (Developer settings) твоего телефона есть пункт OEM unlock, а ты не собираешься в ближайшее время разблокировать загрузчик — отключи его.
4. Если в твоем телефоне есть настройка режима, в котором устройство должно быть доступно при подключении к компьютеру, выбери «Только зарядка» (Charge only). В противном случае из твоего заблокированного телефона удастся скопировать содержимое карты памяти, включая фото и видео. Если такой настройки нет, то проверь, что происходит при подключении. Как правило, в современных устройствах режим Charge only будет выбран по умолчанию. Если это так — все в порядке; если же по умолчанию выбран File Transfer или MTP — на безопасности можно ставить крест.
5. Конечно, последняя версия Android — это хорошо, а актуальные патчи безопасности и вовсе вещь обязательная. Проблема лишь в том, что подавляющее большинство производителей безобразно затягивает с обновлениями, оставляя найденные уязвимости незакрытыми на многие месяцы (а то и годы). Если твой телефон не актуальный флагман (или актуальный флагман Samsung или LG), то о быстрых обновлениях можно забыть. Но обновления все равно проверь.

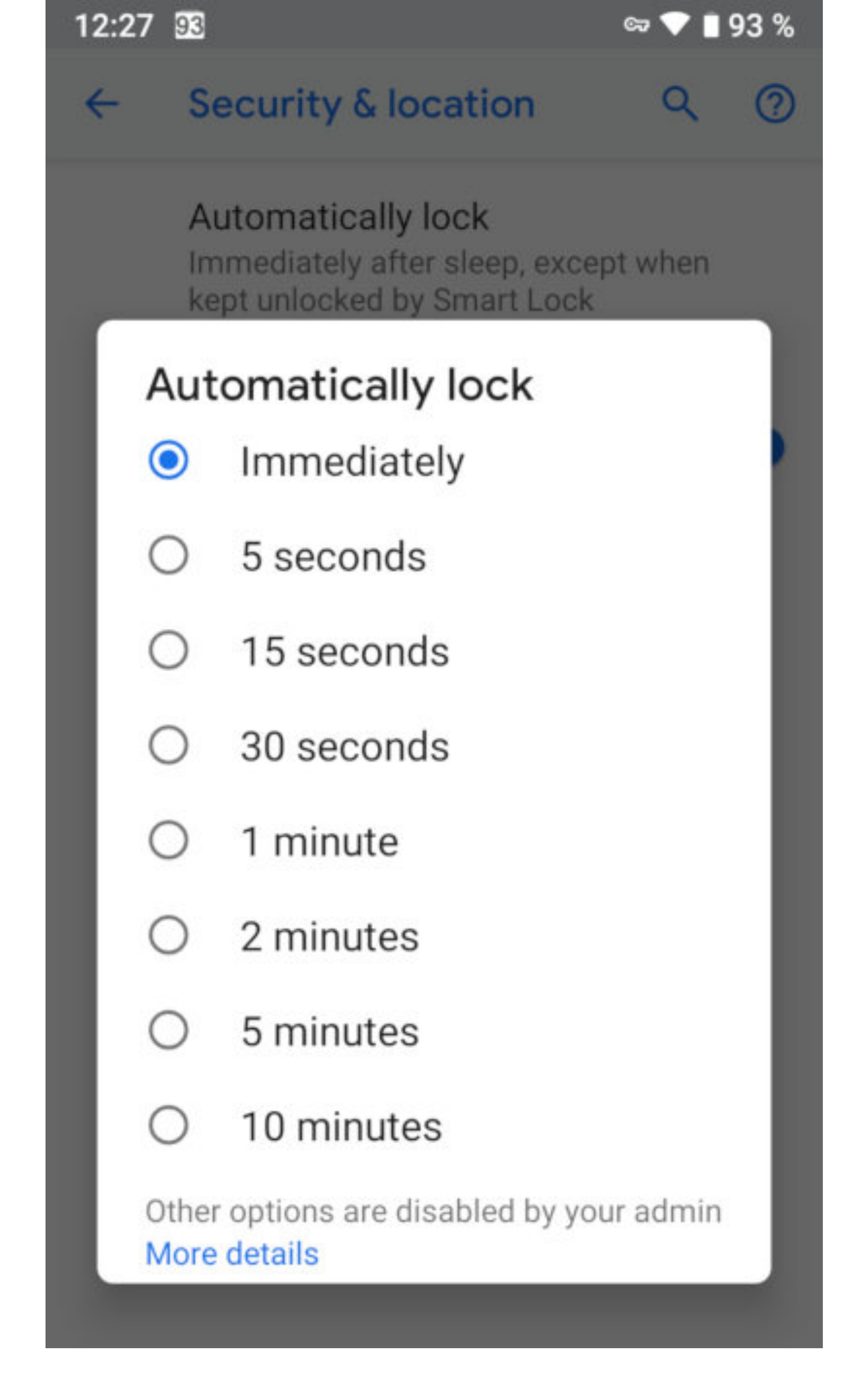
6. Smart Lock — абсолютное зло с точки зрения безопасности. Отключи все виды Smart Lock, в том числе разблокировку по лицу (только в Smart Lock; если твой телефон оборудован объемным сканером с инфракрасной подсветкой — совет неактуален).
7. Заодно отключи задержку блокировки телефона, если она настроена (настрой Settings → Security & Location → Automatically lock → Immediately).
8. Про установку из неизвестных источников не забыл? Не стоит держать этот переключатель в активном состоянии, он действительно делает твой телефон уязвимым. Кстати, в Android 8 отдельной настройки нет; разрешение выдается отдельным приложениям, управлять настройкой можно через пункт настроек Special app access.
9. Буквально на днях произошел скандал: оказалось, что ряд приложений для iPhone записывает действия пользователя и передает в виде аналитики скриншоты экрана, включая персональные данные, номера паспортов и кредитных карт. В Android скандала не было: абсолютно любое приложение с разрешениями Draw over other apps или запущенное в виде сервиса Accessibility может проделать то же самое. Проверь, нет ли там чего лишнего.
10. А еще есть такая вещь, как Device admin. Приложения из этой категории могут использоваться для того, чтобы дистанционно сменить код блокировки, заблокировать или разблокировать устройство, сбросить настройки к заводским. Если это Google Find My Phone или Exchange Admin, установленный твоим работодателем, то все хорошо. Проверь, чтобы в списке не оказалось лишнего.
11. Про встроенные производителями бэкдоры ты, наверное, уже в курсе. Многие производители встраивают в прошивки своих телефонов средства для сбора аналитики. Время от времени оказывается, что «аналитика» — это и твои контакты с паролями. По большому счету, поделать тут особо ничего нельзя. Ты можешь попытаться ограничить доступ аналитики в интернет (например, приложением AdGuard, установленным, кстати, из сторонних источников — с сайта разработчика, а не из Play Store), но если у тебя на руках такой аппарат, то все возможные данные уже давно утекли. Просто смирись.
12. Наконец, о приложениях из Play Store. Многие из них затребовали (и, скорее всего, получили) самые дикие разрешения. Например, «Птичкам» ты мог дать доступ к камере, микрофону и контактам (зачем?), продвинутому калькулятору — доступ к местоположению, а красивой фотогалерее — разрешение на чтение и отправку SMS. Не поленись и зайди в список

разрешений приложений; для большинства пользователей простой анализ выданных разрешений становится большим сюрпризом.

13. Не храни пароль от Google Account в браузере Chrome. Его будут искать в первую очередь.
14. Включи двухфакторную аутентификацию. Без комментариев; на эту тему мы писали не раз и не два.

Отложенная блокировка

Когда-то давно ввод кода блокировки был единственным, медленным и неудобным способом разблокировать экран телефона. Многим пользователям постоянный ввод пароля представлялся неудобным; они отказывались от защиты в пользу удобства и скорости. Отложенная блокировка стала логичной реакцией на проблему со стороны как Google, так и Apple.

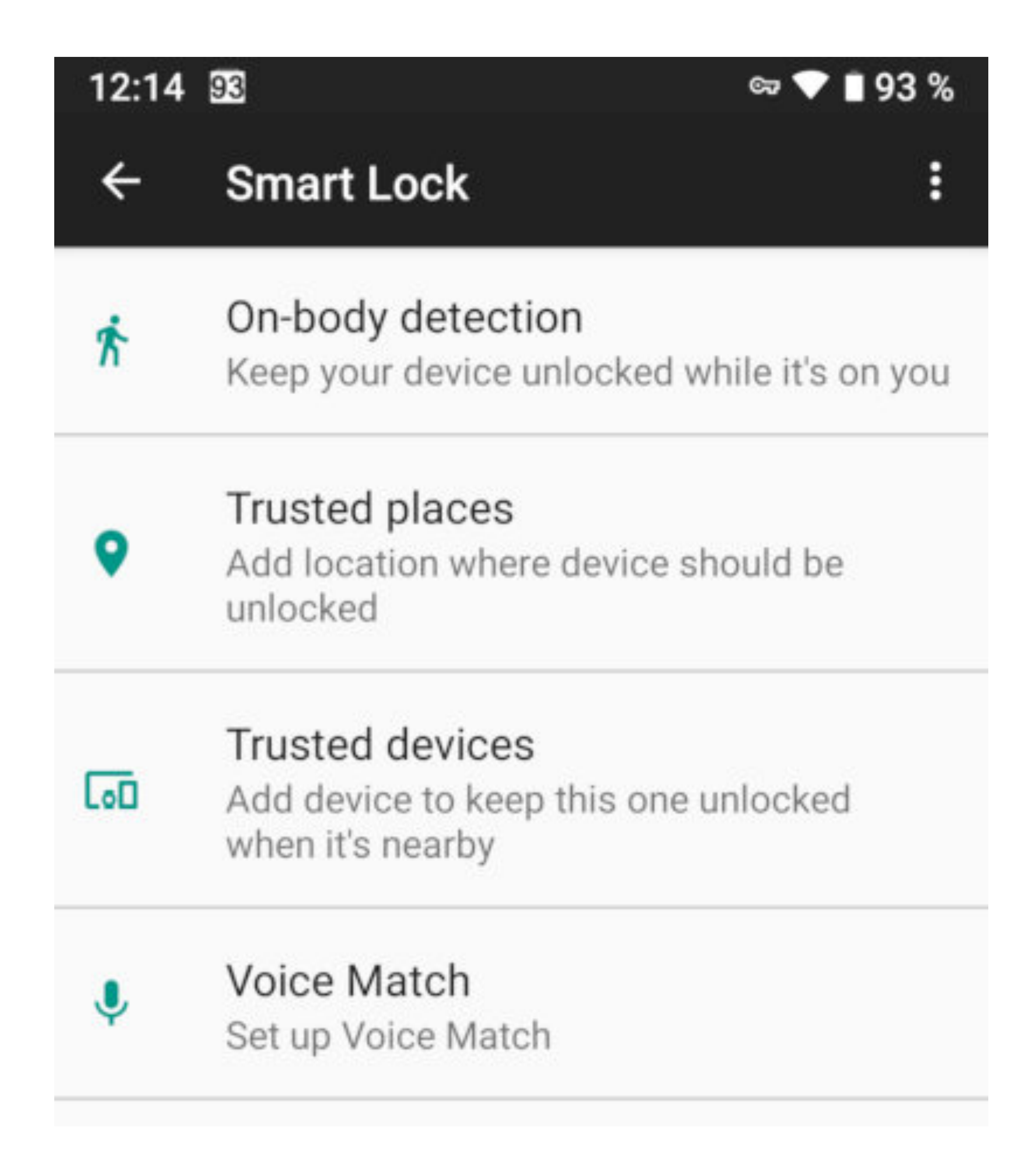


При активации соответствующей опции можно было отключить дисплей телефона кнопкой, включить его снова — и попасть сразу на домашний экран. Задержку можно настраивать в зависимости от собственных предпочтений. Нужно ли говорить, что задержка блокировки катастрофически снижает уровень безопасности? Представь ситуацию: ты идешь по улице, уткнувшись в телефон, и вдруг упираешься в грудь полицейского. Рефлекторно жмешь кнопку отключения дисплея, после чего тебя задерживают. Телефон у тебя конфискуют, включают экран — и сразу же попадают на домашний экран. Пароли, коды блокировки, заблокированный загрузчик, шифрование и многие другие вещи уже не будут иметь значения.

В iOS есть аналогичная настройка: Settings → Touch ID & Passcode → Require Passcode. Ее предназначение примерно такое же, как в смартфонах с Android, за одним важным отличием: если ты используешь Touch ID или Face ID, в современных версиях iOS единственным доступным вариантом выбора будет Immediately (то есть блокировать сразу после отключения экрана). А вот если ты отключишь биометрику, оставив только код блокировки, то станут доступными и другие варианты вплоть до Never (запрашивать код блокировки только после первой загрузки и время от времени согласно постоянно меняющимся политикам Apple). Обрати внимание: некоторые варианты могут быть недоступны, если на твоем устройстве установлена внешняя политика безопасности.

Smart Lock

Почему все так ополчились на функцию Smart Lock? Дело в том, что эта функция позволяет разблокировать телефон, используя методы, которые не имеют ничего общего с безопасностью. Рассмотрим на примерах.



Face unlock. Разблокировка по лицу в разделе Smart Lock не имеет ничего общего с биометрической аутентификацией. Это — всего лишь сличение образа пользователя с фотографией, сделанной на фронтальную камеру устройства. Такой face unlock легко обманывается плоской фотографией. Обрати внимание: в телефонах, оборудованных

биометрической функцией Face Unlock (например, Xiaomi Mi 8), этого пункта в настройках не будет; в таких устройствах Face Unlock подчиняется тем же требованиям и правилам, что и разблокировка по датчику отпечатка пальцев.

Trusted places. Автоматически разблокирует устройства в окрестностях тех мест, где ты часто бываешь. Если телефон вытащат из твоего кармана возле дома, у злоумышленника не возникнет никаких проблем с его разблокировкой.

Trusted devices. Если подключено доверенное устройство Bluetooth, телефон может быть разблокирован автоматически. Поверь, у полиции не возникнет затруднений использовать твои умные часы или трекер для такой разблокировки.

Voice match, On-body detection. В какой-то степени экспериментальные варианты, позволяющие пользователям реже разблокировать устройство кодом блокировки.

Если Smart Lock настолько небезопасен, почему он вообще есть в Android? Smart Lock — тяжкое наследие тех времен, когда ввод кода блокировки или паттерна был единственным способом разблокировать телефон. Подавляющему большинству пользователей не нравилось, что на разблокировку устройства тратятся драгоценные секунды (а разблокировать телефон в перчатках было той еще задачей); в результате многие не устанавливали никакой защиты вообще. Для того чтобы хоть как-то приучить пользователей к установке кода блокировки, Google пришлось сильно занизить планку: так, появились опции, позволяющие отсрочить блокировку экрана на 10–15 минут с момента последней разблокировки. Smart Lock — из той же оперы. Никакой разумной нужды что в Smart Lock, что в отложенной блокировке уже не осталось: современные сканеры отпечатков пальцев срабатывают чуть быстрее, чем просто «мгновенно», а разблокировка по лицу достигла достаточно высоких уровней скорости и безопасности.

Разблокировка по лицу

Насколько безопасна разблокировка по лицу? Мы не стали писать об этом в разделе про iPhone; в них используется система с достаточным уровнем технической безопасности. В смартфонах с Android производители устанавливают модули разблокировки по лицу, безопасность которых находится в пределах от «хорошо» до «тот же Smart Lock, вид сбоку». Так, в смартфонах Samsung есть режим, комбинирующий образ лица со сканированием радужной оболочки глаза; обмануть такую систему трехмерной моделью головы не удастся. Аналогичные системы стали появляться во флагманских устройствах Huawei, Xiaomi и многих других. В то же время в ряде устройств используются гораздо более примитивные системы, основанные или на фотографии с фронтальной камеры, или на двумерном фото с инфракрасного датчика. Обмануть такие системы вполне возможно, иногда — очень просто. Как правильно заметили в статье «Разблокировка по лицу — не лучшая идея», подход «Мой

телефон умеет все то же, что и твой iPhone, — и стоит в десять раз меньше!» будет встречаться все чаще.

Особняком стоит правовой аспект разблокировки по лицу. В США был создан ряд прецедентов, регулирующих возможности полиции разблокировать устройство, сканируя лицо подозреваемого. Имеются как положительные (разрешение на разблокировку по лицу было выдано), так и отрицательные (разрешение не было выдано или было выдано неправомерно) прецеденты, и благодаря им установлены достаточно четкие правовые рамки, переходить которые полицейские в большинстве случаев не станут.

В то же время в России мы неоднократно слышали об историях, когда телефон «случайно» поворачивался в сторону задержанного, после чего «сам собой» разблокировался. Доказать, что телефон был разблокирован с нарушением правовых норм, в таких случаях очень тяжело: нательными камерами, как в США, российские полицейские пока не оснащены.

Использовать или не использовать разблокировку по лицу — вопрос открытый, и ответ на него лежит не только в технической области; решать в любом случае тебе. Автор этого текста такую возможность использует.

Безопасность небезопасного

А что можно сделать, если у тебя на руках откровенно «дырявый» телефон с разблокированным загрузчиком или перепрошитый ушлыми продавцами «китаец»? В этом случае говорить о серьезной безопасности, конечно, не приходится, но кое-что ты сделать все-таки сможешь.

Первый и самый простой вариант: у тебя на руках телефон, загрузчик которого разблокирован (например, предыдущим владельцем). Часто подобные ситуации осложняются тем, что на телефоне установлена кастомная прошивка, есть root-доступ, модифицирован системный раздел или и вовсе непонятно, что там творится. В большинстве случаев такой телефон можно вернуть в «заводское» состояние, прошив его на заводскую прошивку (где скачать, посоветуют на XDA или 4PDA), после чего загрузчик можно заблокировать командой

```
fastboot oem lock
```

. Особенно это рекомендуем проделать с китайскими устройствами, на которые хитрые продавцы часто (чаще, чем ты можешь себе представить!) устанавливают прошивки с самыми разнообразными сюрпризами.
Обрати внимание: данная стратегия не сработает со свежими телефонами Xiaomi,

перепрошитыми с китайского стока на «глобальную» версию MIUI. Если ты попробуешь заблокировать загрузчик на таком устройстве, получишь «кирпич», восстановить который может быть очень и очень трудно. Если все-таки решишь попробовать — хотя бы заведи на телефоне Xiaomi Account, чтобы впоследствии, если что-то пойдет не так, ты мог воспользоваться утилитой Mi Unlock для разблокировки загрузчика.

Но что, если загрузчик нельзя заблокировать (так часто бывает на многих китайских устройствах)? Значит, тебе не повезло. Впрочем, если ты приобрел такое устройство, то, вероятно, безопасность — последняя из проблем такого телефона. Теоретически даже на таких устройствах будет работать шифрование, которое не позволит просто так считать данные. На практике же взлом таких устройств обычно не представляет никакой проблемы. Единственное, что ты можешь попытаться сделать, — настроить Secure Startup; в этом режиме ключ шифрования данных будет генерироваться на основе кода блокировки. Достаточно длинный код блокировки увеличит время, которое потребуется на взлом.

Что делать, если ты приобрел телефон, который ведет себя странно? При малейшем подозрении на вредоносное ПО в прошивке зайди в профильную ветку на 4PDA. Вполне вероятно, что ты с такой проблемой не один и на форуме уже есть подробные инструкции по удалению или заморозке малвари.

А что делать, если производитель не выпускает обновлений, а в прошивке прочно прописались зловредные компоненты? Конечно, разумным поступком было бы избавиться от такого устройства, но в реальном мире так мало кто делает. Поэтому рекомендация: попробуй разблокировать загрузчик (хуже уже не станет) и установить на телефон официальную сборку Lineage OS. В официальных сборках Lineage (в отличие от, например, Resurrection Remix) все хорошо и с приватностью, и с шифрованием, и с обновлениями «по воздуху». В зависимости от доступной для твоего устройства версии прошивки может использоваться шифрование как FDE, так и FBE; в первом случае рекомендуем настроить Secure Startup. Если же сборок Lineage нет или разблокировать загрузчик невозможно, то даже ребенку я бы такой телефон отдавать не стал.

Если забрали компьютер

Обсудив защищенность твоих данных в мобильном устройстве, поговорим о том, как анализ компьютера может повлиять на безопасность твоих мобильных устройств. Если эксперт получил доступ к твоему компьютеру, а полнодисковое шифрование (например, посредством BitLocker) ты не используешь, то запуском простой утилиты и одним-двумя ленивыми кликами мышки будут извлечены все логины и пароли от всех твоих учетных записей. Откуда? Из базы данных твоего любимого браузера: Chrome, Mozilla, Edge… Пользуешься менеджером паролей? Если разработка тебя в качестве подозреваемого представляет хоть какой-то интерес, то к базе данных паролехранилки попытаются

подобрать пароль (тут, впрочем, результат не гарантирован).

Что произойдет, когда пароли будут извлечены? В зависимости от того, каким смартфоном ты пользуешься, эксперт запустит еще одно приложение, которое извлечет всю информацию из облака Apple, Google или, к примеру, Samsung. (В скобках: если ты пользуешься смартфоном Samsung, то знаешь ли ты, что именно хранится в соответствующем облаке, даже если ты не включал его сознательно?)

Если ты пользуешься iPhone, из облака можно извлечь:

- резервные копии (кстати, не всегда; если у тебя свежая версия iOS и активирована двухфакторная аутентификация, то резервную копию скачать не удастся. Впрочем, если у тебя остались старые резервные копии, созданные устройствами с iOS 11 или старше, то их извлечь получится. Мораль: посмотри, что у тебя хранится в облаке, и удали ненужные резервные копии!);
- синхронизированные данные: контакты, заметки, календари, закладки браузера Safari и прочее;
- фотографии (если у тебя включен iCloud Photo Library), в том числе недавно удаленные;
- журнал звонков и историю браузера;
- некоторые данные карт;
- если узнают код блокировки твоего телефона или пароль от компьютера Mac, то и все облачные пароли (iCloud Keychain) и данные «Здоровья» (журнал твоей повседневной активности), а также SMS и iMessage.

Пользуешься Android? Google собирает намного больше данных, чем Apple; длиннее и список доступной для извлечения информации:

- резервные копии и данные приложений (кстати, в Android именно в этой категории будут храниться журналы звонков, SMS, а также маркеры аутентификации отдельных приложений);
- синхронизированные данные: календари, контакты, заметки;
- пароли Chrome (какой-либо дополнительной защиты, как в iOS, для них не предусмотрено);
- подробнейшая история местоположения за последние много лет. Пожалуй, на этот пункт будут обращать внимание в первую очередь;
- история браузера и поисковых запросов. Исследуется в обязательном порядке;

- почта Gmail, которую можно использовать, например, для сброса пароля к другим учетным записям.

Исследование облака Google часто дает более интересный результат, чем даже анализ самого смартфона, так как собираются данные не только с конкретного телефона, но и со всех других устройств (в том числе компьютеров), в которых ты вошел в свой Google Account.

Если у тебя телефон Samsung, то можно вытащить еще кое-что из собственного облака Samsung. Мы понимаем, что для многих читателей наличие у Samsung собственного облачного сервиса станет сюрпризом, а то, что в нем, оказывается, хранятся какие-то данные (и ты с этим в какой-то момент успел согласиться), может сильно удивить. В облаке Samsung можно найти:

- резервные копии (интересно, что Samsung сохраняет в облаке не только данные приложений, но и APK);
- фотографии (если ты не приложил осознанных усилий, чтобы отключить синхронизацию фотографий в облако);
- данные Samsung Health;
- резервные копии часов и трекеров Samsung.

Пользователи смартфонов Xiaomi (а также других устройств под управлением MIUI) имеют возможность синхронизировать свои устройства с облаком Mi Cloud (если смартфон «глобальной» версии, то информация сохраняется в дополнение к тому, что сохраняется в Google Account). В облаке Mi Cloud можно найти следующее:

- резервные копии. Здесь достаточно скудно: сохраняются APK и настройки телефона, но не сохраняются данные приложений;
- контакты, SMS;
- фотографии, если ты включил синхронизацию.

Как обезопасить себя от облачных атак? Самые распространенные советы по безопасности, кочующие из одной статьи в другую, оказываются и самыми бесполезными. Ты можешь выбрать длинный и сложный пароль, но извлечение даже самого длинного пароля из встроенного в Chrome хранилища займет те же миллисекунды, что и совсем короткого. Ты можешь включить двухфакторную аутентификацию, но обойти ее будет довольно просто, если эксперт достанет из твоего телефона SIM-карту и использует ее для получения одноразового кода. Более того, если твой браузер залогинен в твой Google Account, можно вытащить cookie, содержащие маркеры аутентификации, — в этом случае не нужен ни одноразовый код, ни пароль, ни даже логин. Это не значит, что двухфакторная аутентификация бесполезна — она вполне эффективна против попыток удаленного взлома. Просто рассчитывать только на

эти меры, если работают грамотные эксперты, нельзя.

Помочь может многослойная защита.

Во-первых, обеспечь физическую безопасность компьютера, включив шифрование системного диска через BitLocker. Кстати, убедись, что ключ шифрования BitLocker Recovery Key не «утек» в облако OneDrive (проверить можно тут) или не сохранился в Active Directory.

Если ты живешь в России, то просто так взять и зашифровать системный диск у тебя не получится. Для того чтобы включить шифрование, тебе нужна как минимум профессиональная редакция Windows и аппаратный модуль доверенной загрузки TPM 2.0. Именно в аппаратном модуле должен храниться сам ключ шифрования, при помощи которого будет зашифрован раздел. Модули TPM 2.0 не получили сертификации ФСБ; соответственно, все продающиеся на территории РФ компьютеры не должны включать этот модуль по умолчанию, даже если он физически распаян на материнской плате. Варианты? Если есть возможность активировать TPM 2.0 в настройках BIOS — сделай это и включи BitLocker. Если такой возможности нет, то разрешить шифрование системного раздела при помощи BitLocker получится и без аппаратного модуля. Сделать это можно вручную, отредактировав групповые политики Windows. Подробности — по ссылке: https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/.

Следующий слой защиты — пароли для облачных учетных записей. Для облачных сервисов Google, Apple, Samsung, Xiaomi используй уникальные пароли, непохожие на все те, что записаны в хранилище браузера. Запусти свой любимый, не самый любимый и совсем нелюбимый браузеры и убедись, что в их хранилище нет данных перечисленных выше учетных записей. Если используешь Chrome — выйди из учетной записи Google. Сотри кеш и куки браузера, после чего закрой все окна. Всё, на какое-то время (пока ты снова не войдешь в Google Account) ты защищен от облачного вектора атаки.

Использование такой системы незначительно повлияет на удобство повседневного использования, но существенно повысит безопасность.

Lockdown

У пользователей iPhone есть дополнительный фактор риска: файл lockdown, он же — iTunes pairing record. Эти файлы создаются при подключении iPhone или iPad к компьютеру, на котором установлено приложение iTunes; они нужны для того, чтобы при помощи iTunes можно было синхронизировать устройство с компьютером без постоянного ввода кода блокировки. С одной стороны, наличие механизма pairing record

— это удобство. С другой — уязвимость. Так, инструменты «Элкомсофт» позволяют использовать файлы lockdown для создания резервной копии телефона, даже если экран заблокирован (но сам телефон был разблокирован хотя бы раз с момента загрузки). Решение GrayKey в тех же условиях и вовсе позволяет создать полный образ файловой системы (правда, пока только для iOS 11).

Как защититься? С одной стороны, можно удалить файлы lockdown с компьютера; на Windows 10 они находятся в папке

```
C:\Users\<username>\AppData\Roaming\Apple Computer\MobileSync\Backup
```

(если ты устанавливал iTunes с сайта Apple) или в папке

```
C:\Users\<username>\Apple\MobileSync\Backup
```

(если ты используешь версию iTunes из Microsoft Store).
А вот просто так удалить эти записи на iPhone нельзя; можно лишь сбросить все доверенные записи сразу через Settings → General → Reset → Reset Location & Privacy. Кстати, для сброса нужно будет ввести код блокировки. Другой способ удалить доверенные записи — сброс настроек Reset Network Settings. А вот Reset All Settings на записи доверия не влияет никак (зато удаляет пароль на резервную копию).

Насколько реальны риски, связанные с анализом компьютера? По информации от самих полицейских, исследование компьютеров проводят нечасто. Как правило, у полиции возникают следующие препятствия:

- препятствия юридического характера: имеющееся постановление разрешает досмотр и анализ улик, имевшихся у задержанного при себе (но не дает разрешения на обыск в квартире);
- ограничения по времени: работа эксперта поставлена на поток. В рутинных случаях у эксперта нет месяца, недели или даже нескольких дней, чтобы подробнейшим образом проанализировать все доступные улики;
- пароль к BitLocker чрезвычайно стойкий. Атаки «в лоб» обречены, если полиция не сможет извлечь готовый ключ шифрования посредством, к примеру, FireWire Attack;
- поверхностная экспертиза: в результате жестких временных рамок содержимое жесткого диска просматривается на предмет вполне конкретных файлов (фото- и видеоматериалы, переписка, базы данных мессенджеров);
- даже если предпринимается полный анализ, очень часто в кеше браузеров не оказывается нужных паролей;
- даже если нужные пароли есть, в облаке подозреваемого не оказывается резервных копий вообще или достаточно свежих резервных копий. Даже для

iOS это типичная ситуация: если оставить все настройки по умолчанию, то мизерные 5 Гбайт бесплатного места в облаке в кратчайшие сроки будут забиты синхронизированными фотографиями. На резервные копии места уже не останется. А вот у пользователей Android — останется: как резервные копии, так и фотографии в «стандартном» качестве не учитываются в и без того достаточно щедрой квоте в 15 Гбайт.

Заключение

В этой статье мы подробно рассмотрели риски и настройки безопасности, выходящие далеко за рамки стандартных советов «установить код блокировки» и «включить двухфакторную аутентификацию». Надеемся, что понимание рисков, связанных с теми или иными твоими действиями и настройками, поможет тебе адекватно оценить степень безопасности твоих данных — и, возможно, укрепить слабые места без каких-либо заметных неудобств в работе устройства.



Олег Афонин

Эксперт по мобильной криминалистике компании «Элкомсофт»



Теги: Android iPhone SmartLock Взлом Выбор редактора Информационная безопасность Облако Смартфоны Статьи Утечка данных